IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants: Moskowitz et al.	Art Unit: 3639
Serial Number: 09/990,842	Examiner: Nelson, Freda
Filing Date: 11/21/2001	Confirmation No.: 2704
Title: SECURE METHOD AND SYSTEM FOR DETERMINING CHARGES AND ASSURING PRIVACY	Docket No.: CHA920010021US1 (IBMC-0038)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS

This is an appeal from the Final Rejection (OA) dated January 31, 2006, rejecting claims 1-6, 8-17, 19-25 and 33-38. The requisite fee set forth in 37 C.F.R. §1.17 (c) has been submitted on March 31, 2006.

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

As filed, this case includes claims 1-38. Claims 1-6, 8-17 and 19-38 remain pending, among which claims 1-6, 8-17, 19-25 and 33-38 stand rejected, and form the basis of this appeal, and claims 26-32 are withdrawn from consideration; claims 7 and 18 are cancelled. No claim has been allowed. The rejections of claims 1-6, 8-17, 19-25 and 33-38 are being appealed.

STATUS OF AMENDMENTS

No amendment has been filed following the Final Rejection of January 31, 2006.

SUMMARY OF THE CLAIMED SUBJECT MATTER

A first aspect of the present invention (e.g., claim 1) provides a system (see, e.g., Figure 1, remote apparatus 10 + central server 12) for processing usage data within a local data processing system (11) installed on a remote apparatus (10), wherein the local data processing system (11) comprises: a sensor (monitoring system 14) for gathering usage data from the remote apparatus (10) (page 6, lines 6-7); and a processor (16) for processing the gathered usage data and calculating a charge based on the gathered usage data (page 6, lines 10-11), wherein a security system (18) comprises an encryption system for encrypting usage data transmitted between the sensor and the processor (page 6, lines 12-14 and page 11, lines 3-9).

A second aspect of the present invention (e.g., claim 16) provides a system (see, e.g., Figure 1, remote apparatus 10 + central server 12) for managing usage data collected on a remote apparatus (10), comprising: a local data processing system (11) having: a

monitoring system (14) for gathering usage data from the remote apparatus (page 6, lines 6-7); a processor (16) for processing the usage data (page 6, lines 10-11); a communications system (20) for communicating the processed usage data (page 6, lines 15-16); and a security system (18) for securing the usage data, wherein the security system includes an encryption system for encrypting usage data communicated from the monitoring system to the processor (page 6, lines 12-14 and page 11, lines 3-9).

A third aspect of the present invention (e.g., claim 23) provides a system (remote apparatus 10 + central server 12) for managing usage information collected on a remote apparatus (10), comprising: a central server (12) for receiving information from the remote apparatus (10) (page 6, lines 15-16), and processing (24) the information to obtain a usage payment (page 7, lines 16-18); and a local data processing system (11) installed on the remote apparatus (10), having: a monitoring system (14) for gathering usage data from the remote apparatus (10) (page 6, lines 6-7); a processor (processing system 16) for managing the usage data (page 6, lines 10-11); a communications system (20) for communicating information from the processor (16) to the central server (12) (page 6, lines 15-16); and a security system (18), wherein the security system includes an encryption system for securing information transmitted to the central server (page 14, lines 11-16), and for securing information processed by the central server (12) (page 15, line 17 – page 16, line 13).

A forth aspect of the present invention (e.g., claim 33) provides a method for managing usage data collected on a remote apparatus (10), comprising: providing a sensor (14) on the remote apparatus (10) to gather usage data (page 6, lines 6-7); communicating (wireless or wired transmission; page 10, lines 6-17) the usage data to a

processor (16) located on the remote apparatus (10); calculating a charge on the processor (16) based on the usage data (page 6, lines 10-11 and page 6, line 23); and communicating the charge to a server (12) via a wireless transmission channel (page 7, line 10-13; page 6, line 15-16).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-2, 8, 10, 12, 14, and 33 are unpatentable under 35 USC 103(a) over Dar et al. (US Publication 2001/0039509), hereinafter "Dar," in view of Van De Pavert (USPN 5,914,471), hereinafter "Van De Pavert."

2. Whether claims 3-5, 15-17, 19-21 and 23 are unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, further in view of Ando et al. (USPN 5,955,970), hereinafter "Ando."

3. Whether claim 6 is unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of Ando, still in further view of Force et al. (USPN 5,533,123), hereinafter "Force";

4. Whether claim 9 is unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of Ando, still in further view of Force, and still in further view of Davis et al. (USPN 5,844,986), hereinafter "Davis."

5. Whether claim 11 is unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, still in further view of Ehrman et al. (US Publication 2001/0037298), hereinafter "Ehrman."

6. Whether claim 13 is unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of McMillan et al. (US Patent 6,064,970), hereinafter "McMillan."

7. Whether claims 22 and 24-25 are unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, still in further view of Ando, still in further view of Ehrman.

8. Whether claims 34-35 and 37-38 are unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of Shimizu et al. (US Publication 2002/0111822), hereinafter "Shimizu."

9. Whether claim 36 is unpatentable under 35 USC 103(a) over Dar in view of Van De Pavert, in further view of Shimizu, still in further view of Ehrman.

ARGUMENT

1. Claims 1-2, 8, 10, 12, 14, and 33 are not obvious over Dar in view of Van De Pavert.

Appellants submit that the suggested combinations of the cited prior art do not disclose or suggest each and every claimed feature. For example, with respect to claims

1 and 33, Appellants submit that Dar and Van De Pavert do not disclose or suggest, *inter alia*, "communicating the usage data to a processor located on the remote apparatus; [and] calculating a charge on the processor based on the usage data[.]" (Claim 33, emphasis added; similarly claimed in claim 1). The Office alleges that this feature is taught in paragraph 0039 of Dar in which billing data is provided. (*See* OA at p5). However, a careful reading of paragraph 0039 clearly reveals that the billing data is provided by a data processor that is not located on the vehicle, but at a central unit. As detailed, e.g., in paragraph 0157 of Dar, the billing system resides at the central unit. In view of the foregoing, Dar fails to teach or suggest a system that calculates a charge on the processor that is "located on the remote apparatus." Appellants submit that Van De Pavert does not overcome, *inter alia*, this deficiency of Dar. Actually, in the Final Office Action, the Office does not provide a reason/explanation how and why Van De Pavert is used in the rejection of claim 33.

With further regard to claims 1 and 33, the claimed invention includes, *inter alia*, "a security system (located on remote apparatus) comprises an encryption system for encrypting usage data transmitted between the sensor and the processor." (Claim 1, parenthetical explanation added). As the Office admits, Dar does not disclose or suggest this feature. (*See* OA at p4.) However, Appellants submit that Van De Pavert also does not disclose or suggest, *inter alia*, this feature. In Van De Pavert, the communication of card data is between a card and a secure module 3 of a card operated device 2 (FIG. 2). Neither the card nor the secure module 3 of Van De Pavert gathers usage data from a remote apparatus because neither is a sensor to gather a usage of the telephone, e.g., a timer. The card or the secure module 3 only exchanges data that are already stored in the

card. As such, the encryption of Van De Pavert does not disclose or suggest encrypting usage data transmitted between a sensor that gathers usage data and a processor.

The above arguments also apply to cryptographic circuitry 54 of Van De Pavert (FIG. 4) because the device (card) of FIG. 4 is only an implementation of the FIG. 2 module using "commercially available components," and cryptographic circuitry 54 does not encrypt usage data transmitted between a sensor that gathers usage data and a processor.

Moreover, in Van De Pavert, block 125 (FIG. 3A) does not encrypt usage data, based on which the processor calculates a charge. Rather, in Van De Pavert, "block 125 executes a pre-defined cryptographic process to encrypt this code and the associated card data on which the code is based[,]" in a verification procedure. (Col. 9, lines 5-7, emphasis added). In Van De Pavert, the card data "includes … a value of the current card balance[.]" (Col. 8, lines 64-65). However, in the verification procedure of Van De Pavert, a card balance is not a usage data because a use of the card has not taken place. A card balance at this stage may reflect previous usage, but the previous usage will not be used as a basis for calculating a current charge. Actually, Van De Pavert expressly discloses that "this procedure (including encryption) will not take place after each successive adjusting (e.g., reduction) of a card balance." (Col. 8, lines 5-6, parenthetical explanation added). As such, Van De Pavert does not encrypt a usage data, e.g., time of use.

In the OA, the Office asserts that "Van De Pavert teaches enciphering can be used both [*sic.*] in order to transmit the usage (balances) in a secure manner." (OA at p2). Appellants respectfully disagree because as discussed above, a starting balance of a card

in the verification procedure of Van De Pavert does not reflect a usage based on which a charge is calculated. In view of the foregoing, Dar and Van De Pavert, even in suggested combination, do not disclose or suggest "an encryption system for encrypting usage data transmitted between the sensor and the processor[,]" as claimed in the claimed invention.

In view of the foregoing, Appellants respectfully submit that claims 1 and 33 are allowable over the art of record.

Claims 2, 8, 10, 12, 14 are allowable for the reasons stated above for claim 1, as well as for their own additional features.

2. Claims 3-5, 15-17, 19-21 and 23 are not obvious over Dar, Van De Pavert and Ando.

2-1 With respect to claim 16, the above arguments also apply. Appellants submit that Ando does not overcome, *inter alia*, the above-identified deficiencies of Dar and Van De Pavert because Ando does not encrypt usage data transmitted between the sensor that gathers the usage data and the processor. The Office asserts that Ando discloses "a security system for protecting monetary data stored therein and ensuring legitimate communication with the stationary device." (OA at p5). Appellants respectfully submit that this assertion is irrelevant in this case because the current invention claims "an encryption system for encrypting usage data transmitted between the sensor and the processor (in the same local data processing system)." (Claim 1, parenthetical explanation added). In Ando, the communication is between an on-board device 20 and a stationary device 60, which are not in the same local data processing system within the

remote apparatus. In view of the foregoing, Appellants respectfully submit that claim 16 is allowable over the art of record.

2-2 With respect to claim 23, the claimed invention recites, *inter alia*, "a security system, wherein the security system includes an encryption system for securing information transmitted to the central server, and for securing information processed by the central server." (Emphasis added). The Office Action alleges that the combination of Dar, Van De Pavert and Ando suggests the features of this claim. Appellants respectfully traverse because neither reference teaches or suggests a security system "for securing information processed by the central server." Particularly, in Ando, which is used by the Office to overcome the deficiencies of Dar and Van De Pavert regarding this claim, there is no teaching or suggestion that any information remains or is continually treated secure and encrypted once received and processed by the central server. Accordingly, Appellants submit that claims 23-25 are allowable over the art of record.

Claims 3-5 and 15 are allowable for the same reasons stated above for claim 1, as well as for their own additional features, and Ando does not overcome the deficiencies of Dar and Van De Pavert. Claims 17, 19-21 are allowable for the same reasons stated above for claim 16, as well as for their own additional features.

3. Claim 6 is allowable for the same reasons stated above for claim 1, as well as for its own additional features, and Ando and Force do not overcome the deficiencies of Dar and Van De Pavert.

4. Claim 9 is allowable for the same reasons stated above for claim 1, as well as for its own additional features, and Ando, Force and Davis do not overcome the deficiencies of Dar and Van De Pavert.

5. Claim 11 is allowable for the same reasons stated above for claim 1, as well as for its own additional features, and Ehrman does not overcome the deficiencies of Dar and Van De Pavert.

6. Claim 13 is allowable for the same reasons stated above for claim 1, as well as for its own additional features, and McMillan does not overcome the deficiencies of Dar and Van De Pavert.

7. Claim 22 is allowable for the same reasons stated above for claim 16, as well as for its own additional features, and Ehrman does not overcome the deficiencies of Dar, Van De Pavert and Ando; and 24-25 are allowable for the same reasons stated above for claim 23, as well as for their own additional features, and Ehrman does not overcome the deficiencies of Dar, Van De Pavert and Ando.

8. Claims 34-35 and 37-38 are allowable for the same reasons stated above for claim 33, as well as for their own additional features, and Shimizu does not overcome the deficiencies of Dar and Van De Pavert.

9. Claim 36 is allowable for the same reasons stated above for claim 33, as well as for its own additional feature, and Ehrman does not overcome the deficiencies of Dar and Van De Pavert.

In addition, Appellants submit that by combining multiple, e.g., more than three, references without providing any support that there is reasonable expectation of success founded in the teachings of the references, many of the rejections made by the Office are weak. Appellants respectfully request reversal or reconsideration of those weak rejections.

In view of the foregoing, Appellants submit that the Office has failed to state a *prima facie* case of obviousness in the final rejection, and the Final Rejection should be reversed.

Respectfully submitted,

Dated: 11/3/06

Michael F. Hoffman
Reg. No. 40,019

Hoffman, Warnick & D'Alessandro LLC
75 State Street, 14th Floor
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)

CLAIMS APPENDIX

1. A system for processing usage data within a local data processing system installed on a remote apparatus, wherein the local data processing system comprises:

a sensor for gathering usage data from the remote apparatus; and

a processor for processing the gathered usage data and calculating a charge based on the gathered usage data, wherein a security system comprises an encryption system for encrypting usage data transmitted between the sensor and the processor.

2. The system of claim 1, further comprising a communications system for transmitting the calculated charge to a central server via a wireless transmission channel.

3. The system of claim 2, further comprising a security system, wherein the security system comprises a tamper resistant encasement that encases at least one component of the local data processing system.

4. The system of claim 3, wherein the at least one encased component comprises the processor.

5. The system of claim 3, wherein the at least one encased component comprises the sensor.

6. The system of claim 3, wherein the tamper resistant encasement comprises an epoxy having a signature embedded therein.

8. The system of claim 2, further comprising a security system, wherein the security system comprises an encryption system for encrypting data communicated by the communications system.

9. The system of claim 1, wherein the processor comprises a cryptographic coprocessor.

10. The system of claim 1, wherein the charge comprises an insurance cost.

11. The system of claim 1, wherein the charge comprises a rental cost.

12. The system of claim 1, wherein the remote apparatus is selected from the group consisting of: a vehicle, a boat, an aircraft, a heating system, a home appliance, a medical device, a dwelling, a factory, a commercial establishment, and an insurable object.

13. The system of claim 1, wherein the sensor measures a speed of the apparatus.

14. The system of claim 1, wherein the sensor collects data from a GPS system.

15. The system of claim 1, wherein the sensor measures weight placed on the remote apparatus.

16. A system for managing usage data collected on a remote apparatus, comprising:

a local data processing system having:

a monitoring system for gathering usage data from the remote apparatus;

a processor for processing the usage data;

a communications system for communicating the processed usage data; and

a security system for securing the usage data, wherein the security system includes an encryption system for encrypting usage data communicated from the monitoring system to the processor.

17. The system of claim 16, wherein the security system includes a tamper resistant encasement for securing the processor.

19. The system of claim 16, further comprising a central server for receiving the processed usage data and securing a usage payment, wherein the usage payment is determined from the processed usage data.

20. The system of claim 19, wherein the security system further comprises a second encryption system for encrypting data transmitted between the communications system and the central server.

21. The system of claim 20, wherein the usage payment comprises an insurance payment.

22. The system of claim 20, wherein the usage payment comprises a rental payment.

23. A system for managing usage information collected on a remote apparatus, comprising:

a central server for receiving information from the remote apparatus, and processing the information to obtain a usage payment; and

a local data processing system installed on the remote apparatus, having:

a monitoring system for gathering usage data from the remote apparatus;

a processor for managing the usage data;

a communications system for communicating information from the processor to the central server; and

a security system, wherein the security system includes an encryption system for securing information transmitted to the central server, and for securing information processed by the central server.

24. The system of claim 23, wherein the usage payment comprises an insurance payment.

25. The system of claim 23, wherein the usage payment comprises a rental payment.

33. A method for managing usage data collected on a remote apparatus, comprising:

providing a sensor on the remote apparatus to gather usage data;

communicating the usage data to a processor located on the remote apparatus;

calculating a charge on the processor based on the usage data; and

communicating the charge to a server via a wireless transmission channel.

34. The method of claim 33, further comprising:

obtaining an electronic payment based on the charge.

35. The method of claim 33, wherein the charge is an insurance cost.

36. The method of claim 33, wherein the charge is a rental cost.

37. The method of claim 33, wherein the usage data is encrypted prior to being communicated to the processor.

38. The method of claim 33, wherein the charge is encrypted prior to being communicated to the server.

EVIDENCE APPENDIX

There is no evidence submitted.

RELATED PROCEEDINGS APPENDIX

There is no related proceeding.

CERTIFICATE OF SERVICES

There is no other party to this appeal proceeding.